



Criterios de seguridad mínimos – Fabricantes Extranjeros

Marzo de 2020

Nota: Los números de identificación de los criterios no son secuenciales en todos los casos. Los números de identificación no enumerados no son aplicables a los fabricantes extranjeros.

Primera área de enfoque: La seguridad empresarial

1. **La visión de la seguridad y la responsabilidad –** Para que un programa de seguridad de la cadena de suministro de un miembro de CTPAT entre y permanezca en vigencia, debe contar con el respaldo de la alta dirección de una empresa. Inculcar la seguridad como una parte integral de la cultura de la empresa y asegurarse de que sea una prioridad a nivel de toda la empresa es en gran parte la responsabilidad de los líderes de la empresa.

ID	Criterios	Guía de la implementación	Debe / Debería
1.1	Para fomentar una cultura de seguridad, los miembros de CTPAT deberían demostrar su compromiso con la seguridad de la cadena de suministro y el programa CTPAT mediante una declaración de apoyo. La declaración debería estar firmada por un alto funcionario de la empresa y exhibirse en lugares adecuados de la empresa.	La declaración de apoyo debería enfatizar la importancia de proteger la cadena de suministro de actividades delictivas como el narcotráfico, el terrorismo, el tráfico de personas y el tráfico ilegal. Entre los altos funcionarios de la empresa que deberían apoyar y firmar la declaración se pueden encontrar el presidente, el director general, el gerente general o el director de seguridad. La declaración de apoyo puede colgarse en el sitio web de la empresa, exhibirse en carteles ubicados en lugares clave de la empresa (la recepción, el área de embalado, la bodega, entre otros) o ser parte de los seminarios de seguridad de la empresa, entre otros.	Debería

ID	Criterios	Guía de la implementación	Debe / Debería
1.2	Para desarrollar un programa de seguridad de la cadena de suministro sólido, la empresa debería incorporar representantes de todos los departamentos pertinentes en un equipo multidisciplinario. Estas nuevas medidas de seguridad deberían incluirse en los procedimientos vigentes de la empresa, con lo cual se crea una estructura más sostenible y se enfatiza que la seguridad de la cadena de suministro es la responsabilidad de todos.	La seguridad de la cadena de suministro tiene un alcance mucho más amplio que los programas de seguridad tradicionales. Está ligada con la seguridad, en muchos departamentos como Recursos Humanos, Tecnología de la Información y despachos de Importación/Exportación. Los programas de seguridad de la cadena de suministro formulados sobre la base de modelos más tradicionales de los departamentos de seguridad pueden ser menos viables a largo plazo, ya que la responsabilidad de ejecutar las medidas de seguridad se concentra en menos empleados y esto da lugar a que puedan ser más susceptibles a la pérdida de personal clave.	Debería
1.3	El programa de seguridad de la cadena de suministro se debe diseñar, respaldar e implementar a través de un adecuado componente de revisión por escrito. El propósito de este componente de revisión es documentar que se cuenta con un sistema en vigor mediante el cual el personal rendirá cuentas respecto a sus responsabilidades y que todos los procedimientos de seguridad descritos por el programa de seguridad se están implantando según lo diseñado. El plan de revisión debe actualizarse según sea necesario en función de los cambios pertinentes en las operaciones y el nivel de riesgo de una organización.	El objetivo de una revisión para fines de CTPAT es comprobar que sus empleados están siguiendo los procedimientos de seguridad de la empresa. El proceso de revisión no tiene que ser complejo. El miembro decide el alcance de las revisiones y qué tan profundas serán según su función en la cadena de suministro, el modelo empresarial, el nivel de riesgo y las variaciones entre los lugares o sitios específicos. Las empresas más pequeñas pueden crear una metodología de revisión muy simple, mientras que un conglomerado multinacional grande tal vez necesite un proceso más extenso y también tomar en consideración varios factores como los requisitos legales locales, entre otros. Algunas empresas grandes pueden ya contar con auditores en plantilla que podrían aprovecharse para ayudar con las revisiones de la seguridad. Un miembro puede optar por utilizar revisiones específicas más pequeñas dirigidas a procedimientos específicos. Las áreas especializadas que son clave para la seguridad de la cadena de suministro, como las inspecciones y los controles de sellos, pueden someterse a revisiones específicas de esas áreas. No obstante, es útil llevar a cabo una revisión general en forma periódica para asegurarse de que todas las áreas del programa de seguridad funcionen según lo diseñado. Si un miembro se encuentra desde ya llevando a cabo	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
		revisiones como parte de su revisión anual, ese proceso podría ser suficiente para cumplir con este criterio. Para miembros con cadenas de suministro de alto riesgo (determinadas por su evaluación del riesgo), se pueden incluir en el programa de revisión ejercicios de simulación o ejercicios de mesa para asegurarse de que el personal sepa cómo reaccionar en el caso de un incidente de seguridad real.	
1.4	El punto de contacto (POC) de la empresa con CTPAT debe conocer los requisitos del programa de CTPAT. Estas personas deben proporcionar actualizaciones periódicas a la alta gerencia con respecto a asuntos relacionados con el programa, entre ellos el avance o los resultados de cualquier auditoría, ejercicios relacionados con la seguridad y las validaciones de CTPAT.	CTPAT espera que el POC designado sea una persona que se adelanta a la acción y que se involucre y responda a su especialista en seguridad de la cadena de suministro. Los miembros pueden identificar a otras personas que pueden ayudar a apoyar esta función al indicarlos como contactos en el portal de CTPAT.	Debe

2. **La evaluación del riesgo** – La amenaza continua de grupos terroristas y organizaciones delictivas dirigida a las cadenas de suministro enfatiza la necesidad de que los miembros evalúen la exposición real y potencial a estas amenazas en desarrollo. CTPAT reconoce que cuando una empresa tiene múltiples cadenas de suministro con diferentes socios empresariales, enfrenta una mayor complejidad para asegurar esas cadenas de suministros. Cuando una empresa cuenta con varias cadenas de suministro, se debería enfocar en áreas geográficas o cadenas de suministro que tengan un mayor riesgo.

   Al determinar el riesgo dentro de sus cadenas de suministro, los miembros deben considerar varios factores como el modelo comercial, la ubicación geográfica de los proveedores y otros aspectos que pueden ser exclusivos a una cadena de suministro específica.

Definición clave: Riesgo – La medida del daño potencial de un evento no deseado. Abarca la amenaza, la vulnerabilidad y la consecuencia. Lo que determina el nivel de riesgo es qué tan probable es que una amenaza tenga lugar. Una alta probabilidad de que ocurra un incidente por lo general será equivalente a un nivel de riesgo alto. Puede ser que el riesgo no se elimine, pero se puede mitigar al gestionarlo, mediante la reducción de la vulnerabilidad o el impacto general en la empresa.

ID	Criterios	Guía de la implementación	Debe / Debería
2.1	Los miembros de CTPAT deben llevar adelante y documentar el grado de riesgo en las cadenas de suministro. Los miembros de CTPAT deben realizar una evaluación general del riesgo (RA) para identificar dónde pueden existir vulnerabilidades en la seguridad. La evaluación del riesgo (RA) debe identificar amenazas, evaluar riesgos e incorporar medidas sostenibles para mitigar vulnerabilidades. El miembro debe tener en cuenta los requisitos de CTPAT específicos de la función del miembro en la cadena de suministro.	La evaluación general del riesgo (RA) está conformada por dos partes clave. La primera parte es una autoevaluación de las prácticas, los procedimientos y las políticas de seguridad de la cadena de suministro del miembro dentro de las instalaciones que controla para verificar el cumplimiento de los criterios de seguridad mínimos de CTPAT y una revisión general de la gestión de riesgo. La segunda parte de la RA es la evaluación internacional del riesgo. Esta parte de la RA incluye la identificación de una amenaza geográfica según el modelo comercial del miembro y la función en la cadena de suministro. Al ver el posible impacto de cada amenaza en la seguridad de la cadena de suministro del miembro, el miembro necesita un método para evaluar o diferenciar entre los niveles de riesgo. Un método simple es asignar el nivel de riesgo entre bajo, medio y alto. CTPAT desarrolló la orientación para la Evaluación del Riesgo en Cinco Pasos (*Five Step Risk Assessment*) como una ayuda para llevar a cabo la porción internacional de la evaluación del riesgo de la evaluación general del riesgo del miembro, y se puede encontrar en el sitio web de la Oficina de Aduanas y Protección Fronteriza de los Estados Unidos en https://www.cbp.gov/sites/default/files/documents/CTPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf. Para los miembros con cadenas de suministro extensas, se espera que el enfoque principal sea en áreas de mayor riesgo.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
2.2	La porción internacional de la evaluación del riesgo debería documentar o esquematizar el movimiento de la carga del miembro a través de su cadena de suministro desde el punto de origen hasta el centro de distribución del importador. El esquema debería incluir todos los socios comerciales que participan directa e indirectamente en la exportación o el movimiento de las mercancías. Según corresponda, la esquematización debería incluir cómo se mueve la carga dentro y fuera de las instalaciones de transportes o centros de carga y observar si la carga está "en reposo" en uno de estos lugares durante un período prolongado de tiempo. La carga es más vulnerable cuando está “en reposo”, esperando a ser trasladada al tramo siguiente de su viaje.	Cuando se desarrolla un proceso para esquematizar las cadenas de suministro, las áreas de alto riesgo son las primeras a tomar en consideración. Al documentar el movimiento de toda la carga, el miembro debería considerar todas las partes involucradas que correspondan, incluidas aquellas que solamente estarán gestionando los documentos de importación o exportación, como los agentes de aduanas y otros que pueden no manejar directamente la carga, pero que pueden tener control operativo como los Consolidadores de Mercancía Marítima en Unidades de Transporte (NVOCC) o los Proveedores de Logística de Terceros (3PL). Si cualquier porción del transporte se subcontrata, esto también podría tomarse en consideración porque mientras más capas de partes indirectas haya, mayor es el riesgo que existe. El ejercicio de esquematización implica analizar con mayor profundidad cómo funciona su cadena de suministros. Además de identificar los riesgos, también puede servir para identificar las áreas donde la cadena de suministro es ineficiente, lo cual podría dar lugar a que se encuentren formas de disminuir los costos o los plazos de entrega para recibir los productos.	Debería
2.3	Las evaluaciones del riesgo se deben revisar anualmente, o más frecuentemente, según lo dicten los factores de riesgo.	Las circunstancias que pueden requerir que se revise una evaluación del riesgo con más frecuencia que una vez al año incluyen un mayor nivel de amenaza de un país específico, periodos de intensificación de la alerta, después de un incidente o fallo de la seguridad, cambios en los socios comerciales o cambios en la participación/estructura empresarial como las fusiones y adquisiciones, entre otros.	Debe
2.4	Los miembros de CTPAT deberían contar con procedimientos por escrito que aborden la gestión de crisis, la continuidad comercial, los planes de recuperación de la seguridad y la reanudación comercial.	Una crisis puede incluir la interrupción del movimiento de los datos comerciales debido a un ciberataque, un incendio o el secuestro de un conductor del transportista por parte de personas armadas. Según el riesgo y el lugar donde el miembro opera o de donde obtiene su producción, los planes de contingencia pueden incluir servicios de apoyo o notificaciones de seguridad adicionales, así como el plan para recuperar lo que fue destruido o robado y volver a las condiciones operativas normales.	Debería

3. **<u>Socios comerciales</u> –** Los miembros de CTPAT se relacionan con una variedad de socios comerciales a nivel local e internacional. Para aquellos socios comerciales que manejan directamente la documentación de la carga o de las importaciones y las exportaciones, es fundamental que el miembro garantice que estos socios comerciales tienen implementadas medidas de seguridad apropiadas para proteger las mercancías a lo largo de la cadena de suministro internacional. Cuando los socios comerciales subcontratan ciertas funciones, se agrega una capa adicional de complejidad a la ecuación, la cual se debe tomar en consideración a la hora de realizar un análisis del riesgo de una cadena de suministro.

   Definición clave: Socio comercial – Un socio comercial es cualquier individuo o empresa cuyas acciones pueden afectar la cadena de seguridad de custodia de las mercancías que se importan a los Estados Unidos o se exportan desde ese mismo país mediante la cadena de suministro de un miembro de CTPAT. Un socio comercial puede ser cualquier parte que brinde un servicio para satisfacer una necesidad dentro de la cadena de suministro internacional de una empresa. Estas funciones incluyen todas las partes (tanto directas como indirectas) involucradas en la compra, la preparación del documento, la facilitación, el manejo, el almacenamiento o el movimiento de la carga para un miembro importador o exportador de CTPAT o en su nombre. Dos ejemplos de socios indirectos son los transportistas subcontratados y los almacenes de consolidación en el extranjero, lo cual ha sido organizado por parte de un funcionario o proveedor de logística.

ID	Criterios	Guía de la implementación	Debe / Debería
3.1	Los miembros de CTPAT deben contar con un proceso escrito, basado en el riesgo, para verificar a los nuevos socios comerciales y para vigilar a los socios actuales. Un factor que los miembros deberían incluir en este proceso es el control de las actividades relacionadas con el lavado de dinero y la financiación del terrorismo. Con el fin de ayudar con este proceso, es importante consultar los indicadores de advertencias de CTPAT sobre actividades de lavado de dinero y financiación del terrorismo basadas en el comercio.	Los siguientes son ejemplos de algunos de los elementos de investigación que pueden ayudar a determinar si una empresa es legítima: • Verificación de la dirección de la empresa y el tiempo que ha permanecido en esa dirección; • Investigación en internet sobre la empresa y sus directores; • Verificación de referencias comerciales; y • Solicitud de un historial crediticio. Algunos ejemplos de socios comerciales que deben verificarse son los socios comerciales directos como los fabricantes, los proveedores de productos, los proveedores de servicios o proveedores pertinentes y los proveedores de transporte o logística. Cualesquiera proveedores de servicios o vendedores que estén directamente relacionados con la cadena de suministro de la empresa o que manejen equipos o información sensible también se incluyen en la lista que debe verificarse.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
		Esta lista incluye a los intermediarios o los proveedores de TI contratados. El nivel de profundidad de la verificación depende del nivel de riesgo en la cadena de suministro.	
3.4	El proceso de verificación de los socios comerciales debe tomar en cuenta si el socio es un miembro de CTPAT o un miembro de un programa aprobado de Operador Económico Autorizado (OEA) con un Acuerdo de Reconocimiento Mutuo (MRA) con los Estados Unidos (o un MRA aprobado). La certificación, ya sea de CTPAT o un OEA aprobado, constituye una prueba aceptable para cumplir con los requisitos del programa para socios comerciales, y los miembros deben obtener una prueba de la certificación y continuar vigilando a estos socios comerciales para asegurarse de que mantienen su certificación.	La certificación de CTPAT de los socios comerciales se puede verificar mediante el sistema de interfaz de verificación del estado en el portal de CTPAT. Si la certificación del socio comercial es de un programa de OEA del exterior, conforme un MRA con los Estados Unidos, la certificación OEA del exterior incluirá un componente de seguridad. Los miembros pueden visitar el sitio web de la administración de aduanas del otro país, donde aparecen los nombres de las OEA de dicha administración, o solicitar la certificación directamente a sus socios comerciales. Los MRA de los Estados Unidos vigentes incluyen: Nueva Zelanda, Canadá, Jordania, Japón, Corea del Sur, la Unión Europea (28 Estados miembros) Taiwán, Israel, México, Singapur, la República Dominicana y Perú.	Debe
3.5	Cuando un miembro de CTPAT subcontrata o contrata elementos de su cadena de suministro, debe ejercer la diligencia debida (mediante visitas, cuestionarios y otros) para garantizar que estos socios comerciales tengan implementadas medidas de seguridad que cumplan o superen los criterios de seguridad mínimos (MSC) de CTPAT.	Los importadores y los exportadores tienden a subcontratar una gran parte de sus actividades de la cadena de suministro. Los importadores (y algunos exportadores) constituyen las partes en estas transacciones que por lo general tienen influencia sobre sus socios comerciales y pueden requerir que se implementen medidas de seguridad a lo largo de sus cadenas de suministro, según sea necesario. Para aquellos socios comerciales que no sean miembros de CTPAT ni miembros de MRA aceptados, el miembro de CTPAT ejercerá la diligencia debida para garantizar (cuando tenga la influencia para hacerlo) que estos socios comerciales cumplan con los criterios de seguridad del programa que corresponden. Para verificar el cumplimiento de los requisitos de seguridad, los importadores realizan evaluaciones de seguridad de sus socios comerciales. El proceso para determinar qué tanta información se debe reunir respecto al programa de seguridad de un socio comercial se basa en la	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
		evaluación del riesgo del miembro, y si existen numerosas cadenas de suministro, las áreas de alto riesgo son la prioridad. La determinación de si un socio comercial cumple con los criterios de seguridad mínimos se puede realizar de diferentes maneras. Con base en el riesgo, la empresa puede llevar a cabo una auditoría en sitio en las instalaciones, contratar a un proveedor de servicios o contratista para realizar una auditoría en sitio o utilizar un cuestionario de seguridad. Si se utilizan cuestionarios de seguridad, el nivel de riesgo determinará la cantidad de detalles o las pruebas que deben reunirse. Se podrían requerir más detalles de las empresas ubicadas en áreas de riesgo alto. Si un miembro envía un cuestionario de seguridad a sus socios comerciales, se debe tomar en consideración la solicitud de la siguiente información: •Nombre y cargo de la(s) persona(s) que completan el cuestionario; •Fecha en que se completa el cuestionario; •Firma de la(s) persona(s) que completaron el documento; •*Firma de un alto funcionario de la empresa, un supervisor de seguridad o un representante autorizado de la empresa que certifique la veracidad del cuestionario; •Incorporación de suficientes detalles en las respuestas para determinar el cumplimiento; y •Sobre la base del riesgo, y si lo permiten los protocolos de seguridad locales, la incorporación de pruebas fotográficas, copias de políticas o procedimientos y copias de formularios completados como las bitácoras de los guardias o listas de control de la inspección de los Instrumentos de Tráfico Internacional. *Las firmas pueden ser electrónicas. Si una firma resulta difícil de obtener o verificar, la persona que completa el cuestionario puede dar fe de la validez del cuestionario a través de un correo electrónico y también de que las respuestas y cualquier documento de respaldo fueron aprobados por un gerente o supervisor (se requiere el nombre y el cargo).	

ID	Criterios	Guía de la implementación	Debe / Debería
3.6	Si se identifican debilidades durante las evaluaciones de seguridad de los socios comerciales, se deben abordar de inmediato, y las correcciones se deben implementar de manera oportuna. Los miembros deben confirmar que las deficiencias hayan sido mitigadas mediante pruebas documentales.	CTPAT reconoce que existirán diferentes plazos para hacer correcciones según lo que se necesita para la corrección. La instalación del equipo físico suele tomar más tiempo que un cambio de procedimiento, pero la brecha de seguridad debe abordarse apenas se descubra. Por ejemplo, si el problema es reemplazar una cerca dañada, el proceso de comprar una nueva cerca debe comenzar inmediatamente (abordando así la deficiencia) y la instalación de una nueva cerca (la acción correctiva) debe realizarse tan pronto como sea factible. Según el nivel del riesgo que exista y la importancia de la debilidad que se halle, algunos asuntos podrían requerir atención inmediata. Si, por ejemplo, se trata de una deficiencia que pueda obstaculizar la seguridad de un contenedor, se debe abordar lo más pronto posible. Algunos ejemplos de prueba documental incluyen copias de contratos para más guardias de seguridad, fotografías tomadas de una cámara de seguridad o una alarma de intrusión recién instalada o copias de las listas de control de inspección, entre otros.	Debe
3.7	Para asegurarse de que los socios comerciales siguen cumpliendo con los criterios de seguridad de CTPAT, los miembros deberían actualizar periódicamente las evaluaciones de seguridad de sus socios comerciales o cuando las circunstancias o los riesgos lo requieran.	Las revisiones periódicas de las evaluaciones de seguridad de los socios comerciales son importantes para garantizar la existencia de un programa de seguridad sólido y que opera correctamente. Si un miembro nunca requirió que se hicieran actualizaciones a su evaluación del programa de seguridad de un socio comercial, el miembro no sabría que un programa que una vez fue viable ya no está en funcionamiento, con lo que se pondría en riesgo la cadena de suministro del miembro. La decisión sobre la frecuencia con que se analizará la evaluación de la seguridad de un socio se basa en el proceso de evaluación del riesgo del miembro. Se esperaría que las cadenas de suministro con un riesgo más alto se sometieran a revisiones más frecuentes que las que presentan un riesgo bajo. Si un miembro se encuentra evaluando la seguridad de su socio comercial por medio de visitas personales, podría considerar hacer uso de otros tipos de visitas requeridas. Por ejemplo, capacitar personal en forma cruzada, de manera que aquellos que evalúan el control de calidad también realicen verificaciones de seguridad. Las circunstancias que pueden requerir que la autoevaluación se actualice con mayor frecuencia incluyen un aumento en el nivel de amenaza de un país proveedor, cambios en la ubicación de origen, nuevos socios comerciales de importancia crítica (aquellos que manejan la carga, brindan seguridad a una instalación y otros).	Debería

ID	Criterios	Guía de la implementación	Debe / Debería
3.8	Para los cargamentos que ingresan a los Estados Unidos, si un miembro subcontrata servicios de transporte a otro transportista de carretera, el miembro debe recurrir a un transportista de carretera certificado por CTPAT o a un transportista de carretera que trabaje directamente para el miembro conforme se establezca en un contrato escrito. El contrato debe estipular el cumplimiento de todos los requisitos establecidos en los criterios de seguridad mínimos (MSC).	El transportista debe suministrar una lista de transportistas y conductores subcontratados a las instalaciones en las que recoge y entrega cargas. Todo cambio a la lista de subcontratistas debería comunicarse de inmediato a los socios pertinentes. Al momento de examinar el cumplimiento de los prestadores de servicios, el miembro debería verificar que la empresa subcontratada sea realmente la empresa que transporta las cargas, y que no tiene cargas subcontratadas adicionales sin aprobación. Los miembros deberían limitar la subcontratación de servicios de transporte a sólo un nivel. Si se permiten excepciones para realizar subcontrataciones adicionales, el miembro de CTPAT y el expedidor deberían ser notificados de que la carga fue objeto de otra subcontratación.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
3.9	Los miembros de CTPAT deberían tener un programa de cumplimiento social documentado que, como mínimo, aborde la manera en que la empresa garantiza que las mercancías importadas a los Estados Unidos no fueron extraídas de minas, producidas o elaboradas, total o parcialmente, haciendo uso de formas de trabajo prohibidas, es decir, trabajo forzoso, en cárceles, en condiciones de servidumbre o trabajo infantil en condiciones de servidumbre.	Los esfuerzos del sector privado para proteger los derechos de los trabajadores en sus operaciones y cadenas de suministro pueden fomentar un mayor entendimiento de las leyes y normas laborales y mitigar las malas prácticas laborales. Estos esfuerzos también crean un ambiente para mejores relaciones obrero-patronales y para mejorar la rentabilidad de la empresa. La Sección 307 de la Ley de Aranceles de 1930 (Sección 1307 del Título 19 del Código de los Estados Unidos) prohíbe la importación de mercadería extraída de minas, producida o elaborada, total o parcialmente, en cualquier país extranjero mediante trabajo infantil forzoso o en condiciones de servidumbre. El trabajo forzoso es definido por el Convenio N.º 29 de la Organización Internacional del Trabajo como todo trabajo o servicio exigido a un individuo bajo la amenaza de una pena cualquiera y para el cual dicho individuo no se ofrece voluntariamente. Un programa de cumplimiento social se refiere a una serie de políticas y prácticas mediante las cuales una empresa busca garantizar el máximo cumplimiento de los aspectos de su código de conducta que cubren asuntos sociales y laborales. El cumplimiento social se refiere a cómo una empresa aborda sus responsabilidades para proteger el ambiente, así como también la salud, la seguridad y los derechos de sus empleados, las comunidades en las que opera, y las vidas y comunidades de los trabajadores a lo largo de sus cadenas de suministro.	Debería

4. **La ciberseguridad** – En el mundo digital de hoy, la ciberseguridad es la clave para salvaguardar los activos más preciados de la empresa: la propiedad intelectual, la información de los clientes, los datos comerciales y financieros, y los registros de los empleados, entre otros. Con una mayor conectividad a la internet existe el riesgo de una violación de los sistemas de información de la empresa. Esta amenaza atañe a empresas de todo tipo y tamaño. Las medidas para proteger la tecnología de la información (TI) y los datos de la empresa son de vital importancia, y los criterios indicados proporcionan una base para un programa general de ciberseguridad para los miembros.

Definiciones clave: Ciberseguridad – La ciberseguridad es la actividad o proceso que se enfoca en proteger las computadoras, las redes, los programas y los datos del acceso, el cambio y la destrucción no deseados o no autorizados. Es el proceso de identificar, analizar, evaluar y comunicar un riesgo cibernético y aceptarlo, evitarlo, traspasarlo o mitigarlo a un nivel aceptable, tomando en consideración los costos y beneficios involucrados.

Tecnología de la Información (TI) – La tecnología de la información comprende las computadoras, el almacenamiento, las redes y otros dispositivos físicos, la infraestructura y los procesos para crear, procesar, almacenar, garantizar e intercambiar todas las formas de datos electrónicos.

ID	Criterios	Guía de la implementación	Debe / Debería
4.1	Los miembros de CTPAT deben contar con políticas o procedimientos de ciberseguridad integrales y por escrito para proteger los sistemas de tecnología de la información (TI). La política escrita de TI debe cubrir, como mínimo, todos los criterios individuales de la ciberseguridad.	Se insta a los miembros a seguir los protocolos de la ciberseguridad que se basan en normas o marcos reconocidos de la industria. El *Instituto Nacional de Normas y Tecnología (NIST) es una de las organizaciones que proporciona un Marco de Ciberseguridad (https://www.nist.gov/cyberframework) y que ofrece una orientación voluntaria sobre la base de las normas, directrices y prácticas existentes para ayudar a manejar y reducir los riesgos de la ciberseguridad tanto interna como externamente. Se puede utilizar para ayudar a identificar y priorizar acciones para reducir el riesgo de la ciberseguridad, y es una herramienta para alinear los enfoques tecnológicos, empresariales y de políticas para gestionar dicho riesgo. El Marco complementa el proceso de gestión de riesgos y el programa de ciberseguridad de la organización. En su defecto, una organización sin un programa de ciberseguridad puede utilizar el Marco como referencia para establecer uno. *NIST es una entidad federal no reguladora adscrita al Departamento de Comercio que promueve y mantiene las normas de medida, y es la entidad desarrolladora de normas de tecnología para el gobierno federal.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
4.2	Para defender los sistemas de Tecnología de la Información (TI) de amenazas de ciberseguridad comunes, una empresa debe instalar suficientes programas de software y equipos para protegerse de programas malignos (virus, programas espías, gusanos y troyanos, etc.) y de intrusiones externas e internas (cortafuegos) en los sistemas de cómputo de los miembros. Los miembros deben asegurarse de que su software de seguridad esté actualizado y reciba actualizaciones de seguridad periódicas. Los miembros deben contar con políticas y procedimientos para prevenir ataques a través de la ingeniería social. Si se da una filtración de datos u otro evento imprevisto provoca la pérdida de datos o equipo, los procedimientos deben incluir una recuperación (o reemplazo) de los sistemas o datos de TI.		Debe

ID	Criterios	Guía de la implementación	Debe / Debería
4.3	Los miembros de CTPAT que utilizan sistemas de redes deben evaluar periódicamente la seguridad de su infraestructura de TI. Si se encuentran vulnerabilidades, las acciones correctivas deben implementarse tan pronto como sea posible.	Una red de cómputo segura es de suma importancia para una empresa y garantizar su protección requiere pruebas periódicas. Esto se puede hacer mediante la programación de escaneos de vulnerabilidad. De la misma manera que un guardia de seguridad revisa si hay puertas y ventanas abiertas en una empresa, un escaneo de la vulnerabilidad (VS) identifica aberturas en sus computadoras (puertos abiertos y direcciones IP), sus sistemas operativos y el software a través del cual un pirata informático podría obtener acceso a los sistemas de TI de la empresa. El VS hace esto comparando los resultados de su análisis con los de una base de datos de vulnerabilidades conocidas y produce un informe de correcciones para que la empresa tome medidas. Existen muchas versiones gratuitas y comerciales disponibles de escáneres de vulnerabilidad. La frecuencia de las pruebas dependerá de varios factores que incluyen el modelo de negocio y el nivel de riesgo de la empresa. Por ejemplo, se deben realizar pruebas cada vez que hay cambios en la infraestructura de la red de una empresa. No obstante, los ciberataques están aumentando entre empresas de todos los tamaños, y esto debe tomarse en consideración a la hora de diseñar un plan de pruebas.	Debe
4.4	Las políticas de ciberseguridad deberían abordar cómo un miembro comparte información sobre amenazas de ciberseguridad con el gobierno y otros socios comerciales.	Se insta a los miembros a compartir información sobre amenazas de ciberseguridad con el gobierno y los socios comerciales dentro de la cadena de suministro. El intercambio de información es una parte clave de la misión del Departamento de Seguridad Nacional para crear una conciencia situacional compartida de la actividad cibernética maliciosa. Los miembros de CTPAT pueden optar por hacerse miembros del Centro Nacional de Integración de Ciberseguridad y Comunicaciones (NCCIC: https://www.us-cert.gov/nccic). El NCCIC comparte información entre socios del sector público y privado para crear conciencia sobre las vulnerabilidades, los incidentes y las mitigaciones. Los usuarios de sistemas de control cibernético e industrial pueden suscribirse a productos de información, fuentes (*feeds*) y servicios informáticos sin costo alguno.	Debería

ID	Criterios	Guía de la implementación	Debe / Debería
4.5	Debe existir un sistema para identificar el acceso no autorizado a los sistemas o datos de TI o el abuso de políticas y procedimientos, incluido el acceso inadecuado a los sistemas internos o sitios web externos y la manipulación o alteración de los datos comerciales por parte de los empleados o contratistas. Todos los infractores deben estar sujetos a las acciones disciplinarias correspondientes.		Debe
4.6	Las políticas y los procedimientos de ciberseguridad se deben revisar anualmente, o con mayor frecuencia, según lo establezcan el riesgo o las circunstancias. Después de la revisión, las políticas y los procedimientos se deben actualizar, en caso de ser necesario.	Un ejemplo de una circunstancia que exigiría que se lleve a cabo una actualización de la política antes del año es un ataque cibernético. Utilizar las lecciones aprendidas del ataque ayudaría a fortalecer la política de ciberseguridad de un miembro.	Debe
4.7	El acceso del usuario debe restringirse según la descripción del trabajo o las tareas asignadas. El acceso autorizado se debe revisar periódicamente para garantizar que el acceso a sistemas sensibles se base en los requisitos del trabajo. El acceso a las computadoras y la red debe eliminarse tras la separación del empleado de la empresa.		Debe

ID	Criterios	Guía de la implementación	Debe / Debería
4.8	Las personas con acceso a los sistemas de Tecnología de la Información (TI) deben usar cuentas asignadas individualmente. El acceso a los sistemas de TI debe protegerse de la infiltración mediante el uso de contraseñas fuertes, frases secretas u otras formas de autenticación, y el acceso del usuario a los sistemas de TI debe estar protegido. Las contraseñas o frases secretas se deben cambiar tan pronto sea posible si existen indicios o sospecha razonable de que están comprometidas.	Para proteger los sistemas de TI de infiltraciones, se debe proteger el acceso del usuario mediante un proceso de autenticación. Las contraseñas o frases de acceso complejas para iniciar sesión, las tecnologías biométricas y las tarjetas de identificación electrónicas son tres tipos diferentes de procesos de autenticación. Se prefieren los procesos que usan más de una medida. Estos se conocen como la autenticación de dos factores (2FA) o la autenticación multifactor (MFA). La MFA es la más segura porque requiere que un usuario presente dos o más pruebas (credenciales) para autenticar la identidad de la persona durante el proceso de inicio de sesión. Las MFA pueden ayudar a cerrar las intrusiones de redes que han sido vulneradas a consecuencia de contraseñas débiles o credenciales robadas. Las MFA pueden ayudar a cerrar estos vectores de ataques al exigir a las personas que fortalezcan las contraseñas o frases secretas (algo que usted sabe) con algo que ellas poseen, como un token o una característica física: una prueba biométrica. Si se utilizan contraseñas, estas deben ser complejas. La publicación especial 800-63B del Instituto Nacional de Normas y Tecnología (NIST): Directrices de la identidad digital (*Digital Family Guidelines*), incluye directrices para el uso de contraseñas (https://pages.nist.gov/800-63-3/sp800-63b.html). Se recomienda el uso de frases secretas largas y fáciles de recordar, en vez de palabras con caracteres especiales. Estas frases secretas más largas (el NIST recomienda permitir hasta 64 caracteres de longitud) se consideran mucho más difíciles de descifrar porque están formadas por una oración o frase fácil de memorizar.	Debe
4.9	Los miembros que permiten que sus usuarios se conecten de forma remota a una red deben emplear tecnologías seguras, como redes privadas virtuales (VPN) para permitir que los empleados accedan a la intranet de la empresa de forma segura cuando se encuentran fuera de la oficina. Los miembros también deben tener procedimientos diseñados para evitar el acceso remoto de usuarios no autorizados.	Las VPN no son la única opción para proteger el acceso remoto a una red. La autenticación multifactor (MFA) es otro método. Un ejemplo de autenticación multifactor sería un token con un código de seguridad dinámico que el empleado debe ingresar para acceder a la red.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
4.10	Si los miembros permiten que los empleados utilicen dispositivos personales para realizar el trabajo de la empresa, todos esos dispositivos deben cumplir con las políticas y procedimientos de seguridad cibernética de la empresa con respecto a incluir actualizaciones de seguridad periódicas y un método para acceder de manera segura a la red de la empresa.	Los dispositivos personales incluyen medios de almacenamiento como discos compactos (CD), reproductores de video (DVD) y unidades de memoria USB. Se debe tener cuidado si se permite a los empleados conectar sus dispositivos personales a sistemas individuales, ya que estos dispositivos de almacenamiento de datos pueden estar infectados con programas malignos que podrían propagarse a través de la red de la empresa.	Debe
4.11	Las políticas y los procedimientos de seguridad cibernética deberían incluir medidas para evitar el uso de productos tecnológicos falsificados o con licencias inapropiadas.	El software informático es propiedad intelectual que le pertenece a la entidad que lo creó. Sin el permiso expreso del fabricante o del publicador es ilegal instalar software, independientemente de la manera en que se haya adquirido. Ese permiso casi siempre toma la forma de una licencia del publicador, la cual acompaña las copias del software autorizadas. El software sin licencia tiene más probabilidades de fallar dada la imposibilidad de actualizarlo. Es más propenso a contener programas malignos, los cuales dejan inservibles las computadoras y la información que estas contengan. No se debe esperar garantías ni respaldo técnico para el software que no tiene licencia, lo cual significa que la empresa debe hacerle frente a cualquier falla por su propia cuenta. También hay consecuencias legales para el software sin licencia, incluidas las penas civiles severas y el procesamiento penal. Los piratas de software aumentan los costos para los usuarios del software legítimo y autorizado y disminuyen el capital disponible para invertir en investigación y desarrollo de nuevo software. Sería recomendable que los miembros tengan una política que requiera conservar las etiquetas de la clave de producto y los certificados de autenticidad cuando se compren medios informáticos nuevos. Los CD, DVD y las memorias USB incluyen características de seguridad holográficas que ayudan a garantizar la recepción de productos auténticos y la protección contra las falsificaciones.	Debería

ID	Criterios	Guía de la implementación	Debe / Debería
4.12	Se debería realizar una copia de seguridad de los datos una vez por semana o según sea apropiado. Todos los datos confidenciales y sensibles se deberían almacenar en formato cifrado.	Se debería realizar una copia de seguridad de los datos dado que la pérdida de datos podría afectar a los individuos de la organización en diferente grado. También se recomienda realizar copias de seguridad diarias en caso de que los servidores compartidos o de producción se vean comprometidos o pierdan datos. Los sistemas individuales pueden requerir respaldos menos frecuentes, dependiendo del tipo de información con la que se está trabajando. Los medios utilizados para guardar los respaldos de seguridad deberían guardarse preferiblemente en un lugar fuera de las instalaciones. Los dispositivos utilizados para respaldar los datos no deberían estar en la misma red que la utilizada para el trabajo de producción. El respaldo de los datos en la nube es aceptable como un lugar "fuera de las instalaciones".	Debería
4.13	Todos los medios, hardware u otro equipo de TI que contengan información sensible respecto al proceso de importación y exportación deben contabilizarse mediante la realización periódica de inventarios. Cuando se descarten, se deben vaciar o destruir adecuadamente de acuerdo con las Directrices del Instituto Nacional de Normas y Tecnología (NIST) para la Limpieza de Medios u otras directrices de la industria apropiadas.	Algunos tipos de medios informáticos son los discos duros, las unidades extraíbles, los discos CD-ROM o CD-R, DVD o las unidades USB. El Instituto Nacional de Normas y Tecnología (NIST) ha desarrollado las normas de destrucción de medios de datos del gobierno. Se aconseja a los miembros consultar las normas del NIST para limpiar y destruir equipos y medios informáticos. Limpieza de los medios informáticos: https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization	Debe

Segunda área de enfoque: Seguridad del transporte

5. **<u>La seguridad de los medios de transporte y los Instrumentos de Tráfico Internacional</u>** – Los esquemas del tráfico ilegal a menudo suponen la modificación de los medios de transporte y los Instrumentos de Tráfico Internacional (IIT) o el ocultamiento de tráfico ilegal dentro de los IIT. Esta categoría de criterios cubre las medidas de seguridad diseñadas para prevenir, detectar o impedir la alteración de las estructuras de los IIT o la entrada subrepticia en ellos, lo que podría permitir la introducción de material o personas no autorizadas.

En el momento de llenar o cargar, deben existir procedimientos para inspeccionar los IIT y sellarlos adecuadamente. La carga en tránsito o "en reposo" está bajo menos control y, por lo tanto, es más vulnerable a la infiltración, por lo que los controles de sellado y los métodos para rastrear la carga o transporte en tránsito constituyen criterios clave de la seguridad.

Las violaciones en las cadenas de suministro ocurren con mayor frecuencia durante el proceso de transporte; por lo tanto, los miembros deben estar atentos a que estos criterios clave de carga se cumplan en todas sus cadenas de suministro.

Definición clave: Instrumentos de Tráfico Internacional (IIT) – Los IIT comprenden los contenedores, las plataformas planas, los elementos unitarios de carga (ULD), las camionetas de elevación, las camionetas de carga, los tanques, los contenedores, los patines, las paletas, los paneles de calafateo, los contendedores para textiles u otros contenedores especializados que llegan (cargados o vacíos) en uso o para ser utilizados en el envío de mercadería en comercio internacional.

ID	Criterios	Guía de la implementación	Debe / Debería
5.1	Los medios de transporte y los Instrumentos de Tráfico Internacional (IIT) deben guardarse en un área segura para evitar el acceso no autorizado, lo que podría generar una alteración de la estructura de un Instrumento de Tráfico Internacional o (según corresponda) permitir que el sello o las puertas se vean comprometidos.	El almacenamiento seguro de los medios de transporte y los Instrumentos de Tráfico Internacional (tanto vacíos como llenos) es importante para evitar el acceso no autorizado.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
5.2	El proceso de inspección de CTPAT debe tener procedimientos por escrito tanto para las inspecciones agrícolas, como las de seguridad.	Con el predominio de los esquemas de tráfico ilegal que suponen la modificación de los medios de transporte o los Instrumentos de Tráfico Internacional, es fundamental que los miembros realicen inspecciones de los medios de transporte y de los Instrumentos de Tráfico Internacional para descubrir plagas visibles y deficiencias estructurales graves. Del mismo modo, la prevención de la contaminación de plagas a través de medios de transporte y los IIT es de suma importancia, por lo que se ha agregado un componente agrícola al proceso de inspección de seguridad. La contaminación por plagas se define como formas visibles de animales, insectos u otros invertebrados (vivos o muertos, en cualquier etapa del ciclo de vida, incluidas las cáscaras de los huevos o los huevecillos) o cualquier material orgánico de origen animal (entre ellos la sangre, los huesos, el pelo, la carne, las secreciones, las excreciones); plantas o productos vegetales viables o no viables (entre ellos las frutas, las semillas, las hojas, las ramitas, las raíces, la corteza) u otro material orgánico, incluidos los hongos; o la tierra o el agua; cuando dichos productos no son la carga manifestada dentro de los instrumentos de tráfico internacional (por ejemplo, los contenedores, los elementos unitarios de carga y otros).	Debe
5.3	Los miembros de CTPAT deben garantizar que se realicen las inspecciones de seguridad y agrícolas sistemáticas de CTPAT a continuación. Los requisitos para estas inspecciones variarán según si la cadena de suministro es terrestre (Canadá o México) o si la cadena de suministro se origina en el extranjero (modalidades oceánica y aérea). Antes de llenar o empacar, todos los Instrumentos de Tráfico Internacional (IIT) vacíos deben someterse a inspecciones y los medios de transporte también deben someterse a inspecciones cuando cruzan fronteras terrestres para ingresar a los Estados Unidos.	Todos los medios de transporte y los Instrumentos de Tráfico Internacional (IIT) se someten a inspecciones de seguridad y agrícolas para garantizar que sus estructuras no se hayan modificado para ocultar el tráfico ilegal ni se hayan contaminado con plagas agrícolas visibles. Las expectativas para las cadenas de suministro en el extranjero comprenden inspeccionar todos los instrumentos de IIT en el punto de llenado o empaque. Sin embargo, si una cadena de suministro oceánica o aérea presenta mayor riesgo, puede justificar la inclusión de procedimientos de inspección más extensos que abarquen los medios de trasporte o inspecciones en	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
	Requisitos de inspección para los cargamentos de CTPAT vía oceánica, aérea y transfronteriza (conforme corresponda) por flete ferroviario o intermodal: Se debe realizar una inspección de siete puntos en todos los contenedores vacíos y los elementos unitarios de carga (ULD), así como también una inspección de ocho puntos en todos los ULD y los contenedores refrigerados vacíos: 1. La pared frontal; 2. El lado izquierdo; 3. El lado derecho; 4. El piso; 5. La parte superior o el techo; 6. Las puertas interiores y exteriores, incluida la fiabilidad de los mecanismos de bloqueo de las puertas; 7. El exterior o el bastidor; y 8. La caja del ventilador en contenedores refrigerados. Requisitos de inspección adicionales para cruces fronterizos terrestres por transportistas de carretera: Las inspecciones de los medios de transporte y los IIT deben realizarse en los patios de almacenamiento. Siempre que sea posible, se deben realizar inspecciones al entrar y salir de los patios de almacenamiento y en el punto de carga o llenado. Estas inspecciones sistemáticas deben incluir inspecciones de 17 puntos: **Tractores:** 1. Parachoques, llantas, aros;	terminales portuarias marinas o instalaciones de logística aérea. Usualmente, los niveles de riesgo son más altos en los cargamentos con cruces terrestres, por lo que tanto los medios de transporte como los IIT se someten a inspecciones múltiples. Algunos ejemplos de IIT para varias modalidades son contenedores oceánicos, contenedores o remolques refrigerados, remolques de carretera, remolques de plataforma plana, contenedores cisterna, automotores o vagones cubiertos, tolvas y elementos unitarios de carga (ULD). La sección de la biblioteca pública del portal CTPAT contiene material de capacitación sobre la seguridad y los medios de transporte e Instrumentos de Tráfico Internacional agrícolas.	

ID	Criterios	Guía de la implementación	Debe / Debería
	2. Puertas, compartimientos de herramientas y mecanismos de bloqueo; 3. Caja de la batería; 4. Respirador de aire; 5. Tanques de combustible; 6. Compartimentos interiores de la cabina o litera; 7. Techo. **<u>Remolques</u>**: 1. Área de la quinta rueda: se debe revisar la placa de deslizamiento o el compartimento natural; 2. El exterior - frontal y lateral; 3. La parte trasera – parachoques o puertas; 4. La pared frontal; 5. El lado izquierdo; 6. El lado derecho; 7. El piso; 8. La parte superior o el techo; 9. Las puertas interiores o exteriores y los mecanismos de bloqueo; y 10. El exterior y el bastidor.		

ID	Criterios	Guía de la implementación	Debe / Debería
5.4	Los medios de transporte y los Instrumentos de Tráfico Internacional (según corresponda) deben estar equipados con hardware externo que pueda resistir razonablemente los intentos de retirarlo. La puerta, las manijas, las varillas, los cerrojos, los remaches, los soportes y todas las demás partes del mecanismo de bloqueo de un contenedor deben inspeccionarse por completo para detectar la manipulación y cualquier discrepancia en el hardware antes de colocar cualquier dispositivo de sellado.	Considere el uso de contenedores o remolques con bisagras resistentes a la manipulación. Los miembros también pueden colocar placas protectoras o barras de metal en al menos dos de las bisagras de las puertas o colocar un sello o cinta adhesiva sobre al menos una bisagra en cada lado.	Debe
5.5	La inspección de todos los medios de transporte y los Instrumentos de Tráfico Internacional vacíos deberían registrarse en una lista de control. Los siguientes elementos deberían documentarse en la lista de control: • El número de contenedor, remolque o Instrumentos de Tráfico Internacional; • La fecha de inspección; • La hora de inspección; • El nombre del empleado que realiza la inspección; y • Las áreas específicas de los Instrumentos de Tráfico Internacional que se inspeccionaron. Si las inspecciones son supervisadas, el supervisor también debería firmar la lista de control. La hoja de inspección completa de los contenedores o Instrumentos de Tráfico Internacional debería ser parte del paquete de la documentación del embarque. El consignatario debería recibir el paquete completo de la documentación del embarque antes de recibir la mercadería.		Debería

ID	Criterios	Guía de la implementación	Debe / Debería
5.6	Todas las inspecciones de seguridad deberían realizarse en un área de acceso controlado y, de ser posible, deberían vigilarse por medio de un sistema de circuito cerrado de televisión (CCTV).		Debería
5.7	Si se encuentra contaminación por plagas visible durante la inspección de los medios de transporte o Instrumentos de Tráfico Internacional, se debe proceder al lavado y la aspiración para eliminar dicha contaminación. Se debe conservar la documentación por un año para demostrar el cumplimiento de estos requisitos de inspección.	El mantenimiento de registros sobre los tipos de contaminantes que se encontraron, dónde se encontraron (lugar en el medio de transporte) y cómo se eliminó la contaminación por plagas son medidas útiles que pueden ayudar a los miembros a evitar la contaminación futura por plagas.	Debe
5.8	Según el riesgo, el personal de administración debería realizar inspecciones aleatorias de los medios de transporte después de que el personal de transporte haya realizado las inspecciones de los medios de transporte o los Instrumentos de Tráfico Internacional. Las inspecciones en los medios de transporte deberían realizarse periódicamente, con una frecuencia mayor según el riesgo. Deberían realizarse aleatoriamente sin previo aviso, de forma que no sean predecibles. Deberían llevarse a cabo en varios lugares donde los medios de transporte son susceptibles: el patio del transportista, después de cargar el camión, y en ruta hacia la frontera de los Estados Unidos.	Las inspecciones de supervisión de los medios de transporte se realizan para contrarrestar las conspiraciones internas. Como práctica recomendada, los supervisores pueden ocultar un artículo (como un juguete o una caja de colores) en el medio del transporte para determinar si el examinador de pruebas de campo o el operador de medios de transporte lo encuentra. El miembro del personal supervisor podría ser un gerente de seguridad, a quien se le hace responsable ante la alta gerencia por la seguridad, u otro miembro del personal de administración designado.	Debería
5.14	Los miembros de CTPAT deberían trabajar con sus proveedores de transporte para dar seguimiento a los medios de transporte desde el punto de origen hasta el destino final. Los requisitos específicos para el seguimiento, la presentación de la información y el intercambio de datos deberían incorporarse en los términos de los contratos de servicio con los proveedores del servicio.		Debería

ID	Criterios	Guía de la implementación	Debe / Debería
5.15	Los expedidores deberían tener acceso al sistema de vigilancia de flota por GPS de su transportista, de manera que puedan seguir el movimiento de sus cargamentos.		Debería
5.16	Para cargamentos fronterizos terrestres que están cerca de la frontera de los Estados Unidos, se debería implementar una política de "no parar" con respecto a las paradas no programadas.	La carga en reposo es carga en riesgo. Las paradas programadas no estarían cubiertas por esta política, pero tendrían que considerarse en un procedimiento general de seguimiento y vigilancia.	Debería
5.24	En zonas de riesgo alto, e inmediatamente antes de la llegada al cruce fronterizo, los miembros de CTPAT deben incorporar un proceso que contemple una "última verificación" para los cargamentos dirigidos a los EE. UU. con el fin de descartar la presencia de algún indicio de alteración en los medios de transporte o Instrumentos de Tráfico Internacional e inspeccionar visualmente los medios de transporte y el proceso de verificación del sello VVTT. Las inspecciones deberían ser realizadas por individuos debidamente capacitados. V – Ver el sello y los mecanismos de cierre del contenedor y asegurarse de que estén bien; V - Verificar el número de sello contra los documentos del cargamento para comprobar su precisión; T – Tirar del sello para asegurarse de que esté colocado correctamente; T – Girar y dar vuelta al sello de perno para asegurarse de que sus componentes no se desatornillan ni se separan unos de otros y de que ninguna parte del sello está floja.		Debería
5.29	Si se descubre una amenaza creíble (o detectada) para la seguridad de un cargamentos o medio de transporte, el miembro debe alertar (tan pronto como sea posible) a todo socio comercial en la cadena de suministro que pueda verse afectado, así como a las fuerzas del orden, según corresponda.		Debe

6. **La seguridad del sellado –** El sellado de los remolques y contenedores, que incluye la integridad continua del sellado, sigue siendo un elemento crucial de una cadena de suministro segura. La seguridad del sello implica contar con una política integral escrita del sellado que aborde todos los aspectos de la seguridad del sellado; la utilización de los sellos correctos de acuerdo con los requisitos de CTPAT, la colocación correcta un sello en un IIT y la verificación de que el sello se ha colocado correctamente.

ID	Criterios	Guía de la implementación	Debe/ Debería
6.1	Los miembros de CTPAT deben contar con procedimientos detallados y por escrito sobre el sellado de alta seguridad. Estos procedimientos deben describir cómo se emiten y controlan los sellos en las instalaciones y durante el tránsito. Los procedimientos deben proporcionar los pasos a seguir si un sello está alterado, ha sido manipulado o tiene un número de sello incorrecto, incluso la documentación del evento, los protocolos de comunicación a los socios y la investigación del incidente. Los hallazgos de la investigación se deben documentar y cualquier acción correctiva debe implementarse lo más rápido posible. Estos procedimientos escritos deben mantenerse a un nivel operativo local con el fin de que sean fácilmente accesibles. Los procedimientos deben revisarse al menos una vez al año y actualizarse según sea necesario. Los controles por escrito del sellado deben incluir los siguientes elementos: **Control del acceso a los sellos**: • La administración de los sellos está restringida al personal autorizado. • El almacenamiento seguro. **El inventario, la distribución y el rastreo (bitácoras de sellos):** • El registro de la recepción de nuevos sellos. • La emisión de sellos registrados en la bitácora. • El rastreo de sellos en la bitácora. • Solo personal capacitado y autorizado puede colocar sellos en los		Debe

ID	Criterios	Guía de la implementación	Debe/ Debería
	Instrumentos de Tránsito Internacional (IIT). **Control de los sellos en tránsito**: • Al recoger un IIT sellado (o después de parar), se debe verificar que el sello esté intacto sin signos de manipulación, • Se debe confirmar que el número de sello coincide con lo que se indica en los documentos de embarque. **Sellos rotos en el tránsito:** • Si se examina la carga, el número de sello de reemplazo debe registrarse. • El conductor debe notificar inmediatamente al despacho cuando se rompe un sello, indicar quién lo rompió y proporcionar el nuevo número de sello. • El transportista debe notificar inmediatamente a la empresa expedidora, al intermediario y al importador del cambio de sello y el número de sello de reemplazo. • El expedidor debe anotar el número del sello de reemplazo en la bitácora de sellos. **Discrepancias de los sellos:** • Se debe conservar cualquier sello alterado o manipulado que se descubra para ayudar en la investigación. • Investigación de la discrepancia; seguimiento con medidas correctivas (si se justifica). • Según corresponda, se debe informar de los sellos comprometidos a la CBP y al gobierno extranjero que corresponda para ayudar en la investigación.		

ID	Criterios	Guía de la implementación	Debe/ Debería
6.2	Todos los cargamentos de CTPAT que pueden sellarse deben protegerse de inmediato después de que la parte responsable cargue, llene o embale (es decir, el expedidor o el embalador en nombre del expedidor) con un sello de alta seguridad que cumpla o supere la norma 17712 más actualizada de la Organización Internacional de Normalización (ISO) para sellos de alta seguridad. Los sellos con pernos y cable que cumplen con los requisitos se aceptan. Todos los sellos que se utilicen deben adherirse de manera segura y adecuada a los Instrumentos de Tráfico Internacional que transportan la carga de los miembros de CTPAT hacia o desde los Estados Unidos.	El sello de alta seguridad utilizado se debe colocar en la posición de la leva de seguridad, si hubiera alguna, en lugar de la manija de la puerta de la derecha. El sello debe colocarse en la parte inferior de la barra vertical más central de la puerta derecha del contenedor. En su defecto, el sello podría colocarse en la manija central de bloqueo más del lado izquierdo en la puerta derecha del contenedor si la posición de la leva de seguridad no se encuentra disponible. Si se utiliza un sello de pernos, se recomienda que el sello de pernos se coloque con la parte o la pieza del barril hacia arriba con la parte del barril por encima del cerrojo.	Debe
6.5	Los miembros de CTPAT (que mantienen inventarios de sellos) deben ser capaces de documentar que los sellos de alta seguridad que usan cumplan o superen la norma ISO 17712 más actualizada.	Una prueba de cumplimiento aceptable es una copia de un certificado de prueba de laboratorio que demuestre el cumplimiento de la norma de la ISO respecto a sellos de alta seguridad. Se espera que los miembros de CTPAT estén al tanto de las características indicativas de manipulación de los sellos que compran.	Debe
6.6	Si un miembro mantiene un inventario de sellos, la administración de la empresa o un supervisor de seguridad debe realizar auditorías de sellos que incluyan un inventario periódico de sellos almacenados y la conciliación contra las bitácoras de inventario de sellos y los documentos de envío. Todas las auditorías deben estar documentadas. Como parte del proceso general de auditoría de sellos, los supervisores de muelles o los administradores de almacenes deben verificar periódicamente los números de sellos utilizados en los medios de transporte y los Instrumentos de Tráfico Internacional.		Debe

ID	Criterios	Guía de la implementación	Debe/ Debería
6.7	Se debe seguir el proceso de verificación del sello de CTPAT para garantizar que todos los sellos de alta seguridad (perno o cable) se hayan colocado correctamente en los Instrumentos de Tráfico Internacional y que estén funcionando según lo diseñado. El procedimiento se conoce como el proceso VVTT: V – Ver el sello y los mecanismos de cierre del contenedor y asegurarse de que estén bien; V - Verificar el número de sello contra los documentos del cargamento para comprobar su precisión; T – Tirar del sello para asegurarse de que esté colocado correctamente; T – Girar y dar vuelta al sello de perno para asegurarse de que sus componentes no se desatornillan ni se separan unos de otros y de que ninguna parte del sello está floja.	Al aplicar sellos de cable, estos deben envolver la base rectangular metálica de las barras verticales para evitar cualquier movimiento hacia arriba o hacia abajo del sello. Una vez que se aplica el sello, asegúrese de que se haya eliminado toda la holgura de ambos lados del cable. El proceso VVTT para los sellos de cable debe garantizar que los cables estén tensos. Una vez que el sello se ha aplicado correctamente, se debe tirar del cable para determinar si hay algún deslizamiento del cable en la pieza de bloqueo (cierre).	Debe

7. **<u>La seguridad de los procedimientos</u> –** La seguridad de los procedimientos abarca muchos aspectos del proceso de importación-exportación, la documentación y los requisitos de la manipulación y el almacenamiento de la carga. Otros criterios de procedimiento de vital importancia se refieren a la notificación de incidentes y la notificación a las fuerzas del orden pertinentes. Además, CTPAT a menudo requiere que los procedimientos se escriban porque ayuda a mantener un proceso uniforme a lo largo del tiempo. No obstante, la cantidad de detalles necesarios para estos procedimientos escritos dependerá de varios elementos, como el modelo comercial de una empresa o el asunto que cubre el procedimiento.

   CTPAT reconoce que la tecnología utilizada en las cadenas de suministro continúa evolucionando. La terminología utilizada a lo largo de los criterios hace referencia a procedimientos escritos, documentos y formularios, pero esto no significa que tengan que estar en papel. Los documentos electrónicos, las firmas electrónicas y otras tecnologías digitales son métodos aceptables para cumplir con estas medidas.

   El programa no está diseñado para ser un modelo de "talla única"; cada empresa debe decidir (en función de su evaluación de riesgos) cómo implementar y mantener los procedimientos. Sin embargo, la incorporación de procesos de seguridad en los procedimientos existentes es más eficaz en lugar de crear un manual separado para protocolos de seguridad. Esto crea una estructura más sostenible y ayuda a enfatizar que la seguridad de la cadena de suministro es responsabilidad de todos.

ID	Criterios	Guía de la implementación	Debe / Debería
7.1	Cuando la carga se realiza durante la noche, o durante un período prolongado de tiempo, se deben tomar medidas para proteger la carga del acceso no autorizado.		Debe
7.2	Las áreas de carga y las áreas circundantes inmediatas deben inspeccionarse periódicamente para garantizar que permanezcan libres de contaminación visible de plagas.	Las medidas preventivas como el uso de cebos, trampas u otras barreras se pueden emplear según sea necesario. La eliminación de malezas o la reducción de la vegetación cubierta de maleza puede ayudar a eliminar el hábitat de las plagas dentro de las áreas de preparación de la carga.	Debe
7.4	La puesta de la carga en contenedores o los IIT debería ser supervisada por un administrador u oficial de seguridad o por otro miembro del personal designado para ello.		Debería

ID	Criterios	Guía de la implementación	Debe / Debería
7.5	Se debería tomar fotografías digitales al momento de cargar el contenedor para tener una prueba documental de la instalación correcta del sello. En la medida de lo posible, estas imágenes deberían enviarse electrónicamente al destino para fines de verificación.	Las pruebas fotográficas pueden incluir imágenes tomadas al momento de cargar para documentar con pruebas las marcas de carga, el proceso de carga, la ubicación donde se colocó el sello y la instalación correcta del sello.	Debería
7.6	Deben existir procedimientos para garantizar que toda la información utilizada en el despacho de la mercaderías o carga sea legible, se encuentre completa, sea precisa y esté protegida ante cambios, pérdidas o la introducción de información errónea, y que se informe a tiempo.		Debe
7.7	Si se utiliza papel, los formularios y otra documentación relacionada con la importación o la exportación deberían protegerse para evitar el uso no autorizado.	Se pueden tomar medidas, como el uso de un archivador con cerrojo, para proteger el almacenamiento de formularios no utilizados, incluidos los manifiestos, con el fin de evitar el uso no autorizado de dicha documentación.	Debería
7.8	La empresa expedidora o su representante debe asegurarse de que el conocimiento de embarque (BOL) o los manifiestos reflejen de manera precisa la información proporcionada al transportista, y los transportistas deben ejercer la diligencia debida para garantizar que estos documentos sean precisos. Los BOL y los manifiestos deben presentarse ante la Oficina de Aduanas y Protección Fronteriza de los EE. UU. (CBP) de forma oportuna. La información del BOL presentada a la CBP debe mostrar el primer lugar o instalación del exterior donde el transportista toma posesión de la carga destinada a los Estados Unidos. El peso y el recuento de piezas deben ser precisos.	Al recoger Instrumentos de Tráfico Internacional sellados, los transportistas pueden confiar en la información provista en las instrucciones de envío de la expedidora. El requisito de imprimir electrónicamente el número de sello en el conocimiento de embarque (BOL) u otros documentos de exportación ayuda a evitar que tenga que seguir cambiando el sello y alterando los documentos pertinentes para que coincidan con el nuevo número de sello. Sin embargo, para ciertas cadenas de suministro, las mercancías pueden ser examinadas en tránsito por una autoridad aduanera de otro país o por la CBP. Una vez que el gobierno rompe el sello, debe haber un proceso para registrar el nuevo número de sello aplicado al IIT después del examen. En algunas ocasiones, se puede escribir a mano.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
7.23	Los miembros de CTPAT deben contar con procedimientos escritos para denunciar un incidente que incluyan una descripción del proceso de escalamiento interno de la instalación. Debe existir un protocolo de notificación para denunciar cualquier actividad sospechosa o incidentes de seguridad (como incautaciones de drogas, descubrimiento de polizones, etc.) que ocurren en cualquier parte del mundo y que afectan a la seguridad de la cadena de suministro del miembro. Cuando corresponda, el miembro debe denunciar todo incidente global a su especialista de seguridad en la cadena de suministro, al puerto de entrada más cercano, a las fuerzas del orden pertinentes y a los socios comerciales que puedan ser parte de la cadena de suministro afectada. Se debe notificar a la CBP tan pronto como sea posible y antes de que cualquier medio de transporte o IIT cruce la frontera. Los procedimientos de notificación deben incluir la información de contacto correcta que indique los nombres y los números de teléfono del personal que requiere una notificación, así como la información de las fuerzas de orden. Los procedimientos deben revisarse periódicamente para garantizar que la información de contacto sea precisa.	Algunos ejemplos de incidentes que justifican la notificación a la Oficina de Aduanas y Protección Fronteriza de los EE. UU. comprenden, entre otros, los siguientes: • Descubrimiento de la manipulación de un contenedor o IIT o del sello de alta seguridad; •Descubrimiento de un compartimento oculto en un medio de transporte o IIT; • La aplicación de un nuevo sello no contabilizado a un IIT; • El tráfico ilegal, incluidas personas; polizones; • La entrada no autorizada en medios de transporte, locomotoras, embarcaciones o portaaviones; • La extorsión, los pagos por protección, las amenazas o la intimidación; • El uso no autorizado de un identificador de entidad comercial (es decir, un número de Importador de Registro (IOR) o un Código Alfa de Transportista Estándar (SCAC) y otros).	Debe
7.24	Deben existir procedimientos para identificar, cuestionar y dirigirse a personas no autorizadas o no identificadas. El personal debe conocer el protocolo para cuestionar a una persona desconocida o no autorizada, saber cómo responder ante la situación y estar familiarizado con el procedimiento a seguir para el retiro de una persona no autorizada de las instalaciones.		Debe

ID	Criterios	Guía de la implementación	Debe / Debería
7.25	Los miembros de CTPAT deberían establecer un mecanismo para denunciar de forma anónima los problemas relacionados con la seguridad. Cuando se recibe una queja, se debería investigar y, si corresponde, tomar las acciones correctivas pertinentes.	Los problemas internos como el robo, el fraude y las conspiraciones internas se pueden denunciar más fácilmente si la parte denunciante sabe que la denuncia se puede hacer de forma anónima. Los miembros pueden establecer un programa de línea directa o un mecanismo similar que permita a las personas permanecer en el anonimato si temen represalias por sus acciones. Se recomienda que cualquier informe se conserve como prueba que respalda que cada uno de los asuntos denunciados fue investigado y que se tomaron acciones correctivas.	Debería
7.27	Toda escasez, excedentes y otras discrepancias o anomalías importantes se deben investigar y resolver, según corresponda.		Debe
7.28	La carga que llega se debe conciliar con la información del manifiesto de carga. La carga de salida se debe verificar contra las órdenes de compra o entrega.		Debería
7.29	Los números de sellos asignados a cargamentos específicos deberían transmitirse al consignatario antes de la salida.		Debería
7.30	Los números de sellos deberían imprimirse electrónicamente en el conocimiento de embarque u otros documentos de envío.		Debería
7.37	Cuando ocurra un incidente de seguridad de importancia, los miembros deben iniciar un análisis posterior al incidente inmediatamente después de tomar conocimiento de este y con el fin de determinar dónde pudo haber estado comprometida la cadena de suministro. Ese análisis no debe obstaculizar ni interferir con ninguna investigación de un organismo de aplicación de la ley del gobierno de la que se tenga conocimiento. Las conclusiones del análisis posterior al incidente que efectúe la empresa deben documentarse, finalizarse tan pronto como sea factiblemente posible, y, si así lo permiten las autoridades de aplicación de la ley, ponerse a disposición de los especialistas en seguridad de la cadena de suministro (SCSS) a solicitud.	Un incidente de seguridad es la violación de las normas de protección en la que se han eludido, evitado o infringido las medidas de seguridad y que deriva en la comisión efectiva o futura de un acto delictivo. Entre los ejemplos de incidentes de seguridad se cuentan los actos de terrorismo, el tráfico ilícito (narcóticos, personas u otros) y la presencia de polizones.	Debe

8. **<u>La seguridad agrícola</u> –** La agricultura es el sector industrial y laboral más grande de los EE.UU. Asimismo, es una industria amenazada por la introducción de contaminantes animales y vegetales extranjeros, como la tierra, el estiércol, las semillas y el material vegetal y animal que puede albergar plagas y enfermedades invasoras y destructivas. La eliminación de contaminantes en todos los medios de transporte y todo tipo de carga puede disminuir las cargas en espera de la CBP, los retrasos y las devoluciones o los tratamientos de las mercancías. Garantizar el cumplimiento de los requisitos agrícolas de CTPAT también ayudará a proteger una industria clave en los Estados Unidos y el suministro de alimentos a nivel mundial en general.

   Definición clave: Contaminación por plagas – La Organización Marítima Internacional define contaminación por plagas como formas visibles de animales, insectos u otros invertebrados (vivos o muertos, en cualquier etapa del ciclo de vida, incluidas las cáscaras de los huevos o los huevecillos) o cualquier material orgánico de origen animal (entre ellos la sangre, los huesos, el pelo, la carne, las secreciones, las excreciones); plantas o productos vegetales viables o no viables (entre ellos las frutas, las semillas, las hojas, las ramitas, las raíces, la corteza) u otro material orgánico, incluidos los hongos; o la tierra o el agua; cuando dichos productos no son la carga manifestada dentro de los instrumentos de tráfico internacional (por ejemplo, los contenedores, los elementos unitarios de carga y otros).

ID	Criterios	Guía de la implementación	Debe / Debería
8.1	Los miembros de CTPAT deben, de acuerdo con su modelo comercial, tener procedimientos por escrito diseñados para evitar la contaminación visible por plagas en conformidad con las reglamentaciones de los Materiales de Embalaje de Madera (WPM). Las medidas visibles de prevención de plagas se deben cumplir en toda la cadena de suministro. Las medidas relacionadas con las reglamentaciones WPM deben cumplir con las Normas	Los WPM se definen como madera o productos de madera (excluidos los productos de papel) utilizados para apoyar, proteger o transportar una mercancía. Los WPM incluyen artículos como paletas, cajones, cajas, carretes y material de estiba. Con frecuencia, estos artículos están hechos de madera no tratada que es posible que no haya sido sometida a un procesamiento o tratamiento suficiente para eliminar o matar las plagas y, por lo tanto, continúa siendo una vía para la introducción y propagación de plagas. Se ha demostrado que el material de estiba en particular presenta un alto riesgo de introducción y propagación de las plagas. La CIPF es un tratado multilateral supervisado por la Organización de las Naciones Unidas para la Alimentación y la Agricultura que tiene como objetivo garantizar una acción coordinada y eficaz para evitar y controlar la introducción y propagación de plagas y contaminantes. La NIMF 15 incluye medidas aceptadas internacionalmente que se pueden aplicar a los WPM para reducir significativamente el riesgo de introducción y propagación de la mayoría de las plagas que pueden estar asociadas con los WPM. La NIMF 15 afecta a todos los materiales de embalaje de madera que requieren ser descortezados y luego tratados térmicamente o fumigados con bromuro de metilo y sellados con la	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
	Internacionales para Medidas Fitosanitarias N.º 15 (NIMF 15) de la Convención Internacional de Protección Fitosanitaria (CIPF).	marca de cumplimiento de la CIPF. Esta marca de cumplimiento se conoce popularmente como el “sello de trigo”. Los productos exentos de la NIMF 15 están hechos de materiales alternativos, como el papel, el metal, el plástico o los productos de paneles de madera (por ejemplo, los tableros de fibra orientada, los tableros duros y la madera contrachapada).	

Tercera área de enfoque: La seguridad física y de las personas

9. La seguridad física –Las instalaciones para el almacenamiento y la manipulación de la carga, las áreas de almacenamiento de los Instrumentos de Tráfico Internacional y las instalaciones donde se prepara la documentación de las importaciones o las exportaciones en emplazamientos locales y en el exterior deben contar con barreras físicas y elementos de disuasión que protejan del acceso no autorizado.

Una de las piedras angulares de CTPAT es la flexibilidad, y los programas de seguridad deberían personalizarse para adaptarse a las circunstancias de cada empresa. La necesidad de seguridad física puede variar mucho según la función del miembro en la cadena de suministro, su modelo comercial y el nivel de riesgo. Los criterios de seguridad física proporcionan un número de elementos disuasivos u obstáculos que ayudarán a evitar el acceso injustificado a la carga, los equipos sensibles o la información, y los miembros deberían emplear estas medidas de seguridad en todas sus cadenas de suministro.

ID	Criterios	Guía de la implementación	Debe / Debería
9.1	Todas las instalaciones para el almacenamiento y la manipulación de la carga, incluidos los patios de remolques y las oficinas, deben tener barreras físicas o elementos de disuasión que impidan el acceso no autorizado.		Debe
9.2	Las cercas perimetrales deberían encerrar las áreas alrededor de las instalaciones para el almacenamiento y la manipulación de la carga. Si una instalación manipula carga, se deberían usar cercas interiores para proteger la carga y las áreas de manipulación de la carga. Según el riesgo, un cercado interior adicional debería separar los varios tipos de carga, como los materiales locales, internacionales, de alto valor o peligrosos. Las cercas deberían ser inspeccionadas periódicamente por personal designado para comprobar la integridad de las mismas y que no tengan daños. Si se encuentran daños en la cerca, las reparaciones deberían hacerse lo antes posible.	Se pueden utilizar otras barreras aceptables en lugar de cercas, como un muro divisorio o elementos naturales que sean impenetrables o que, de otra forma, impidan el acceso, como un acantilado empinado o matorrales densos.	Debería
9.4	Las puertas por donde los vehículos o el personal entran o salen (así como otros puntos de salida) deben ser reforzadas o vigiladas. Las personas y los vehículos pueden estar sujetos a inspecciones de acuerdo con las leyes locales y laborales.	Se recomienda que el número de puertas se mantenga al mínimo necesario para el acceso y la seguridad adecuados. Otros puntos de salida serían las entradas a las instalaciones que no están cercadas.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
9.5	Se debería prohibir que los vehículos de pasajeros privados se estacionen en las áreas de almacenamiento y manipulación de la carga, y de los medios de transporte, o en zonas adyacentes.	Ubique las áreas de estacionamiento fuera de las áreas cercadas u operativas, o al menos a distancias significativas de las áreas de almacenamiento y manipulación de la carga.	Debería
9.6	Se debe proporcionar una iluminación adecuada dentro y fuera de las instalaciones, incluidas, según corresponda, las siguientes áreas: las entradas y las salidas, las áreas de almacenamiento y manipulación de carga, las líneas de las cercas y las áreas de estacionamiento.	Los temporizadores automáticos o los sensores de luz que encienden automáticamente las luces de seguridad apropiadas son complementos útiles a los aparatos de iluminación.	Debe
9.7	La tecnología de seguridad debería utilizarse para vigilar las instalaciones y evitar el acceso no autorizado a las áreas sensibles.	La tecnología de seguridad electrónica utilizada para proteger o vigilar áreas sensibles y puntos de acceso incluye: sistemas de alarma contra robo (perímetro e interior), también conocidos como sistemas de detección de intrusos (IDS); dispositivos de control de acceso y sistemas de videovigilancia (VSS), incluidas las cámaras de circuito cerrado de televisión (CCTV). Un sistema CCTV / VSS podría incluir componentes como cámaras analógicas (de cable coaxial), cámaras basadas en el protocolo de Internet (IP) (de red), dispositivos de grabación y software de gestión de video. Las áreas protegidas o sensibles que se beneficiarían de la videovigilancia pueden incluir: las áreas de almacenamiento y manipulación de la carga, las áreas de envío y recepción donde se conservan los documentos de importación, los servidores de TI, los patios y áreas de almacenamiento para los Instrumentos de Tráfico Internacional (IIT), las áreas donde los IIT se inspeccionan y las áreas de almacenamiento de sellos.	Debería
9.8	Los miembros que dependen de la tecnología de seguridad para la seguridad física deben tener políticas y procedimientos escritos que rijan el uso, el mantenimiento y la protección de esta tecnología.	La tecnología de seguridad necesita probarse periódicamente para garantizar su funcionamiento correcto. Existen directrices generales a seguir:	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
	Como mínimo, estas políticas y procedimientos deben estipular: • Que el acceso a los lugares donde se controla o administra la tecnología se restringe al personal autorizado; • Los procedimientos que se han implementado para probar o inspeccionar la tecnología de manera periódica; • Que las inspecciones incluyen verificaciones de que todo el equipo funciona correctamente y, si corresponde, que el equipo está colocado correctamente; • Que los resultados de las inspecciones y pruebas de desempeño estén documentados; • Que, si las acciones correctivas son necesarias, estas se implementen lo antes posible y que las acciones correctivas tomadas estén documentadas; • Que los resultados documentados de estas inspecciones se conserven durante un tiempo prudencial para fines de auditoría. Si se utiliza una estación de vigilancia central subcontratada (fuera del sitio), el miembro de CTPAT debe contar con procedimientos escritos que estipulen la funcionalidad de los sistemas críticos y los protocolos de autenticación, entre ellos los cambios en el código de seguridad, sumando o restando personal autorizado, las revisiones de contraseña y el acceso o el rechazo a los sistemas. Las políticas y procedimientos de tecnología de seguridad se deben revisar y actualizar anualmente, o con mayor frecuencia, según lo dicte el riesgo o las circunstancias.	• Probar los sistemas de seguridad después de cualquier trabajo de servicio y durante y después de reparaciones, modificaciones o adiciones importantes a un edificio o instalación. El componente de un sistema puede haber sido comprometido, ya sea intencionalmente o no. • Probar los sistemas de seguridad después de cualquier cambio importante en los servicios telefónicos o de internet. Cualquier aspecto que pueda afectar la capacidad del sistema para comunicarse con el centro de vigilancia merece ser revisado con atención. • Asegurarse de que la configuración de video se haya hecho correctamente: grabación activada por movimiento; alertas por detección de movimiento; imágenes por segundo (IPS) y nivel de calidad. • Asegurarse de que los lentes de la cámara (o los domos que protegen las cámaras) estén limpios y que los lentes estén enfocados. La visibilidad no debería estar limitada por obstáculos o luces brillantes. • Hacer pruebas para asegurarse de que las cámaras de seguridad estén colocadas correctamente y permanezcan en la posición correcta (las cámaras pudieron haber sido movidas deliberada o accidentalmente).	

ID	Criterios	Guía de la implementación	Debe / Debería
9.9	Los miembros de CTPAT deberían utilizar recursos con licencia o certificados al considerar el diseño y la instalación de la tecnología de seguridad.	La tecnología de seguridad de hoy día es compleja y evoluciona rápidamente. Muchas veces las empresas compran tecnología de seguridad inadecuada que demuestra ser ineficaz cuando se requiere o pagan más de lo necesario. Buscar la orientación calificada ayudará al comprador a seleccionar las opciones tecnológicas adecuadas para sus necesidades y presupuesto. Según la Asociación Nacional de Contratistas Eléctricos (NECA), en los EE. UU., 33 estados actualmente tienen requisitos de licencia para profesionales dedicados a la instalación de sistemas de seguridad y alarmas.	Debería
9.10	Toda la infraestructura de la tecnología de seguridad debe asegurarse físicamente para evitar el acceso no autorizado.	La infraestructura de la tecnología de seguridad incluye las computadoras, el software de seguridad, los paneles de control electrónico, las cámaras de circuito cerrado de televisión o videovigilancia, los componentes de energía eléctrica y disco duro para cámaras, así como las grabaciones.	Debe
9.11	Los sistemas de la tecnología de seguridad deberían configurarse con una fuente de energía alternativa que permita que los sistemas continúen funcionando en caso de una pérdida inesperada de energía directa.	Un delincuente que trata de violar su seguridad puede intentar desactivar la electricidad de su tecnología de seguridad para circunnavegarla. Por lo tanto, es importante tener una fuente de energía alternativa para su tecnología de seguridad. Una fuente de energía alternativa puede ser una fuente de generación de energía auxiliar o baterías de respaldo. Los generadores de energía de respaldo también se pueden usar para otros sistemas importantes como la iluminación.	Debería

ID	Criterios	Guía de la implementación	Debe / Debería
9.12	Si se hace uso de sistemas de cámaras, las cámaras deberían vigilar las instalaciones y las áreas sensibles para evitar el acceso no autorizado. Las alarmas deberían usarse para alertar a una empresa sobre el acceso no autorizado a áreas sensibles.	Las áreas sensibles, según corresponda, pueden incluir las áreas de almacenamiento y manipulación de la carga, las áreas de envío y recepción donde se conservan los documentos de importación, los servidores de TI, los depósitos de contenedores y las áreas de almacenamiento para los Instrumentos de Tráfico Internacional (IIT), las áreas donde se inspeccionan los IIT y las áreas de almacenamiento de los sellos.	Debería
9.13	Si se hace uso de sistemas de cámaras, las cámaras deben colocarse de forma que cubran áreas clave de las instalaciones que conciernen al proceso de importación o exportación. Las cámaras deberían programarse para grabar a la más alta calidad de imagen razonablemente disponible, y configurarse para grabar las 24 horas del día, los siete días de la semana.	Posicionar las cámaras correctamente es importante para permitir que las cámaras graben tanto como sea posible de la “cadena de custodia” física dentro del control de la instalación. Según el riesgo, las áreas clave pueden incluir el almacenamiento y manipulación de la carga; el envío y la recepción; el proceso de carga, el proceso de sellado; la llegada y salida de los medios de transporte; los servidores de TI; las inspecciones (de seguridad y agrícolas) de los contenedores; el almacenamiento de los sellos y cualquier otra área relacionada con la seguridad de los cargamentos internacionales.	Debe
9.14	Si se hace uso de los sistemas de cámaras, las cámaras deberían tener una función de alarma o notificación, lo que señalaría que hay una “falla de operación o grabación”.	Una falla en los sistemas de videovigilancia podría ser el resultado de que alguien desactive el sistema para violar una cadena de suministro sin dejar prueba en video de la infracción. La función de falla en la operación puede provocar que se envíe una notificación electrónica a las personas previamente designadas indicándoles que el dispositivo requiere atención inmediata.	Debería

ID	Criterios	Guía de la implementación	Debe / Debería
9.15	Si se hace uso de sistemas de cámaras, se deben realizar revisiones aleatorias periódicas de las imágenes de las cámaras (por parte de la administración, la seguridad u otro personal designado) para verificar que los procedimientos de seguridad de la carga se están siguiendo adecuadamente de acuerdo con la ley. Los resultados de las revisiones deben resumirse por escrito para incluir cualquier acción correctiva tomada. Los resultados se deben conservar durante un tiempo prudencial para fines de auditoría.	Si las imágenes de la cámara solo se revisan con causa (como parte de una investigación luego de una violación de seguridad u otros), no se está haciendo uso del beneficio completo que genera la posesión de cámaras. Las cámaras no son solamente herramientas de investigación; si se utilizan de una manera dinámica, pueden ayudar a evitar que ocurra una violación de la seguridad desde el comienzo mismo. El enfoque debe estar en la revisión aleatoria de las imágenes en la cadena de custodia física para garantizar que el cargamento permaneció seguro y que se siguieron todos los protocolos de seguridad. Algunos ejemplos de los procesos que pueden revisarse son los siguientes: • Las actividades de manipulación de la carga; • Las inspecciones de los contenedores; • El proceso de carga; • El proceso de sellado; • La llegada y salida de los medios de transporte; y • La salida de la carga y otros. **Propósito de la revisión:** La revisión es para evaluar el cumplimiento y la eficacia en general de los procesos de seguridad establecidos, para identificar brechas o debilidades percibidas, y para establecer acciones correctivas para respaldar la mejoría de los procesos de seguridad. Según el riesgo (incidentes anteriores o un informe anónimo sobre un empleado que no sigue los protocolos de seguridad en el muelle de carga u otros), el miembro puede fijar periódicamente una revisión.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
		Asuntos que deben incluirse en el resumen escrito: • La fecha de la revisión; • La fecha en que se revisaron las imágenes; • La cámara o el área de donde procede la grabación • Una breve descripción de cualquier hallazgo; y • Las acciones correctivas, si se justifican.	
9.16	Si se utilizan cámaras, se deberían conservar las grabaciones de imágenes que cubren procesos clave de importación o exportación de un cargamento vigilado durante suficiente tiempo para que se pueda completar una investigación.	Si se produjera una violación, sería necesario llevar a cabo una investigación, y conservar todas las imágenes de las cámaras que cubrían el embalado (para exportación) y los procesos de carga o sellado serían de suma importancia para descubrir dónde se pudo haber comprometido la cadena de suministro. El programa CTPAT recomienda asignar al menos 14 días después de que el cargamento vigilado haya llegado al primer punto de distribución, donde el contenedor se abre por primera vez después del despacho aduanero.	Debería

10. **<u>Los controles del acceso físico</u> –** Los controles de acceso impiden el acceso no autorizado a las instalaciones y áreas, ayudan a mantener el control de los empleados y visitantes, y protegen los activos de la empresa. Los controles de acceso incluyen la identificación positiva de todos los empleados, visitantes, proveedores de servicios y proveedores en todos los puntos de entrada.

ID	Criterios	Guía de la implementación	Debe / Debería
10.1	Los miembros de CTPAT deben tener procedimientos por escrito que regulen cómo se otorgan, cambian y retiran las credenciales de identificación y los dispositivos de acceso. Cuando corresponda, debe existir un sistema de identificación de personal para fines de identificación positiva y control de acceso. El acceso a las áreas sensibles debe restringirse según la descripción del trabajo o las tareas asignadas. El retiro de los dispositivos de acceso debe llevarse a cabo tras la separación del empleado de la empresa.	Los dispositivos de acceso incluyen las credenciales de identificación para los empleados, las credenciales temporales para visitantes y proveedores, los sistemas de identificación biométrica, tarjetas de proximidad, los códigos y las claves. Cuando se separa a los empleados de una empresa, el uso de listas de control de salida ayuda a asegurar que todos los dispositivos de acceso hayan sido devueltos o desactivados. Para las empresas más pequeñas, donde el personal se conoce, no se requiere ningún sistema de identificación. En general, para una empresa con más de 50 empleados, se requiere un sistema de identificación.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
10.2	Los visitantes, vendedores y proveedores de servicios deben presentar una identificación con fotografía a su llegada, y se debe mantener una bitácora que registre los detalles de la visita. Todos los visitantes deberían ser escoltados. Además, todos los visitantes y proveedores de servicios deberían recibir una identificación temporal. Si se utiliza una identificación temporal, debe estar visible en todo momento durante la visita. La bitácora de registro debe incluir lo siguiente: • Fecha de la visita; • Nombre del visitante; • Verificación de una identificación con fotografía (del tipo verificado, como licencia de conducir o tarjeta nacional de identidad). Los visitantes frecuentes y conocidos, como los vendedores habituales, pueden pasar sin la identificación con fotografía, pero siempre se debe registrar su ingreso y salida de la instalación; • Hora de llegada; • Punto de contacto en la empresa; y • Hora de salida.		Debe
10.3	Los conductores que entregan o reciben la carga deben identificarse positivamente antes de recibir o liberar la carga. Los conductores deben presentar una identificación con fotografía emitida por el gobierno al empleado de la instalación que otorgue acceso a fin de verificar su identidad. Si no es factible presentar una identificación con fotografía emitida por el gobierno, el empleado de la instalación puede aceptar una forma reconocible de identificación con fotografía emitida por la empresa transportista de carretera que emplea al conductor que recoge la carga.		Debe

ID	Criterios	Guía de la implementación	Debe / Debería
10.4	Se debe mantener una bitácora de recolección de carga para registrar a los conductores y registrar los detalles de sus medios de transporte al recoger la carga. Cuando los conductores llegan para recoger la carga en una instalación, un empleado de la instalación debe registrarlos en la bitácora de recolección de carga. Cuando los conductores salen, se debe registrar su salida. La bitácora de carga debe mantenerse en un lugar seguro, y los conductores no deben tener acceso a la misma. La bitácora de recolección de carga debería incluir los siguientes puntos: • El nombre del conductor; • La fecha y la hora de llegada; • El patrono; • El número de camión; • El número de remolque; • La hora de salida; • El número del sello colocado al cargamento al momento de la salida.	Una bitácora de visitantes puede tener doble función como bitácora de carga, siempre que la información adicional esté registrada en la misma.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
10.7	Antes de la llegada, el transportista debería informar a la instalación la hora estimada de llegada para la recolección programada, el nombre del conductor y el número de camión. Cuando sea operacionalmente factible, los miembros de CTPAT deberían permitir entregas y recolecciones solamente con cita.	Este criterio ayudará a las expedidoras y a los transportistas a evitar las recolecciones ficticias. Las recolecciones ficticias son esquemas delictivos que dan lugar al robo de carga mediante el engaño, lo que incluye a choferes de camión que usan identificaciones falsas o comercios ficticios establecidos con el propósito de robar carga. Cuando un transportista cuenta con choferes fijos que recogen mercancías de una instalación determinada, una buena práctica es que esta mantenga una lista de los choferes con sus fotografías. Por lo tanto, si no es posible informar a la empresa qué chofer va a venir, la empresa aún podrá verificar que el conductor cuenta con la aprobación para recoger la carga de la instalación.	Debería
10.8	Antes de ser admitidos, los paquetes y el correo que lleguen deberían examinarse periódicamente en busca de tráfico ilegal.	Algunos ejemplos de este tráfico ilegal incluyen, entre otros, explosivos, drogas ilícitas y dinero.	Debería
10.10	Si se utilizan guardias de seguridad, las instrucciones de trabajo para los guardias de seguridad deben estar en las políticas y los procedimientos escritos. La administración debe verificar periódicamente el cumplimiento y la idoneidad de estos procedimientos mediante auditorías y revisiones de las políticas.	Si bien cualquier instalación puede emplear guardias, a menudo se emplean en las plantas de fabricación, los puertos marítimos, los centros de distribución, los patios de almacenamiento para los Instrumentos de Tráfico Internacionales, los centros consolidadores y expedidores.	Debe

11. La seguridad del personal – El recurso humano de una empresa es uno de sus activos más valiosos, pero también puede ser uno de sus eslabones de seguridad más vulnerables. Los criterios de esta categoría se centran en asuntos como el escrutinio de los empleados y las verificaciones previas al empleo. Muchas violaciones de la seguridad son producto de conspiraciones internas, es decir, cuando uno o más empleados conspiran para eludir los procedimientos de seguridad con el fin de permitir una infiltración en la cadena de suministro. Por lo tanto, los miembros deben ejercer la diligencia debida para verificar que los empleados que ostentan cargos de confianza sean personas confiables y fidedignas. Los cargos de confianza incluyen el personal que trabaja directamente con la carga o su documentación, así como el personal involucrado en el control de acceso a áreas o equipos sensibles. Estos cargos incluyen, entre otros, personal de envíos, recepción y correspondencia, los choferes, los despachantes, los guardias de seguridad y cualquier persona involucrada en las asignaciones de la carga, el seguimiento de los medios de transporte o los controles de los sellos.

ID	Criterios	Guía de la implementación	Debe / Debería
11.1	Se debe contar con procesos para evaluar a los futuros empleados, así como para evaluar periódicamente a los empleados actuales. En la medida de lo posible y según lo permita la ley, la información de la solicitud, como el historial de empleo y las referencias, deben verificarse antes de proceder con el empleo.	CTPAT es consciente de que las leyes laborales y de privacidad en ciertos países puede que no permitan que se verifique toda la información de la solicitud. Sin embargo, se espera que se realice la diligencia debida para verificar la información de la solicitud cuando sea posible hacerlo.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
11.2	De acuerdo con las limitaciones legales que correspondan y la disponibilidad de las bases de datos de antecedentes penales, se deben realizar revisiones de los antecedentes de los empleados. Según la sensibilidad del cargo, los requisitos de investigación de los empleados deberían extenderse para los empleados temporales y los contratistas. Una vez empleados, se deberían realizar reinvestigaciones periódicas en función de la causa o la sensibilidad del puesto del empleado. La evaluación de los antecedentes de los empleados debería incluir la verificación de la identidad y los antecedentes penales del empleado, lo cual comprende las bases de datos de la ciudad, el estado, las provincias y el país. Los miembros de CTPAT y sus socios comerciales deberían tener en cuenta los resultados de las verificaciones de los antecedentes, según lo permitido por los estatutos locales, al tomar decisiones de contratación. Las verificaciones de antecedentes no se limitan a la verificación de la identidad y antecedentes penales. En áreas de mayor riesgo, se puede justificar la realización de investigaciones más exhaustivas.		Debería
11.5	Los miembros de CTPAT deben tener un Código de Conducta para los empleados que comprenda las expectativas y defina conductas aceptables. El Código de Conducta debe incluir sanciones y procedimientos disciplinarios. Los empleados y contratistas deben confirmar que han leído y comprendido el Código de Conducta, para lo cual lo firmarán, y esta confirmación se debe conservar en el archivo del empleado para fines de documentación.	El Código de Conducta ayuda a proteger a la empresa e informa a los empleados de las expectativas. Su objeto es formular y mantener una norma de conducta que sea aceptable para la empresa. Ayuda a las empresas a crear una imagen profesional y a establecer una cultura ética sólida. Incluso una empresa pequeña necesita tener un Código de Conducta, pero no necesita ser sofisticado en cuanto al diseño ni contener información compleja.	Debe

12. La educación, la formación y la concientización – Los criterios de seguridad de CTPAT están diseñados para formar la base de un sistema de seguridad en capas. Si se supera una capa de seguridad, otra capa debería evitar una violación de seguridad o alertar a una empresa de una violación. La implementación y el mantenimiento de un programa de seguridad en capas necesita la participación activa y el apoyo de diferentes departamentos y personal vario.

Uno de los aspectos clave para mantener un programa de seguridad es la formación. Educar a los empleados sobre cuáles son las amenazas y la importancia de su función para proteger la cadena de suministro de la empresa es un aspecto importante para el éxito y la resistencia de un programa de seguridad de la cadena de suministro. Además, cuando los empleados entienden por qué existen procedimientos de seguridad, es mucho más probable que se adhieran a ellos.

ID	Criterios	Guía de la implementación	Debe / Debería
12.1	Los miembros deben establecer y mantener un programa de formación y concientización de la seguridad para reconocer y fomentar la concientización de las vulnerabilidades de la seguridad en las instalaciones, los medios de transporte y la carga en cada punto de la cadena de suministro, las cuales podrían ser explotadas por los terroristas o los traficantes de comercio ilegal. El programa de formación debe ser integral y cubrir todos los requisitos de seguridad de CTPAT. El personal en puestos de confianza debe recibir formación especializada adicional orientada a las responsabilidades que tiene el puesto. Uno de los aspectos clave de un programa de seguridad es la formación. Los empleados que entienden por qué existen medidas de seguridad tienen más probabilidades de cumplirlas. Se debe proporcionar formación sobre la seguridad a los empleados de manera periódica, según lo requieran sus funciones y cargos, y los empleados recién contratados deben recibir esta formación como parte de su orientación o inducción al trabajo. Los miembros deben conservar prueba de la formación, como bitácoras de capacitación, hojas de registro (lista) o registros electrónicos de la formación. Los registros de formación deberían incluir la fecha de la formación, los nombres de los asistentes y los temas que se trataron.	Los temas de formación pueden incluir la protección de los controles de acceso, el reconocimiento de las conspiraciones internas y los procedimientos de notificación de actividades sospechosas e incidentes de seguridad. Siempre que se pueda, la formación especializada debería incluir una demostración práctica. Si se realiza una demostración práctica, el instructor debería dar tiempo a los estudiantes para demostrar el proceso. Para los fines de CTPAT, los puestos de confianza incluyen al personal que trabaja directamente con la carga de importación y exportación o su documentación, así como el personal involucrado en el control del acceso a áreas o equipos sensibles. Dichos cargos incluyen, entre otros, personal de envíos, recepción y correspondencia, choferes, despachantes, guardias de seguridad y cualquier persona involucrada en las asignaciones de la carga, el seguimiento de los medios de transporte y el control de los sellos.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
12.2	Los choferes y otros miembros del personal que llevan a cabo inspecciones agrícolas y de seguridad de los Instrumentos de Tráfico Internacional (IIT) y medios de transporte vacíos deben estar formados para inspeccionar sus medios de transporte o IIT tanto para fines de seguridad como agrícolas. La formación de actualización debe llevarse a cabo periódicamente, según sea necesario después de un incidente o violación de seguridad, o cuando haya cambios en los procedimientos de la empresa. La formación en inspecciones debe incluir los siguientes temas: • Señales de compartimientos ocultos; • Tráfico ilegal en compartimentos naturales; y • Señal de contaminación por plagas.		Debe
12.4	Los miembros de CTPAT deberían tener medidas establecidas para verificar que la formación brindada cumpla con todos los objetivos de capacitación.	Entender la formación y ser capaz de utilizar esa formación en el puesto personal (en el caso de los empleados de confianza) es de suma importancia. Exámenes o pruebas cortas, un ejercicio de simulación o simulacro o auditorías frecuentes de los procedimientos, entre otras, son medidas que el miembro puede implementar para determinar la eficacia de la formación.	Debería
12.8	Según corresponda de acuerdo con sus funciones o cargos, el personal debe estar formado en las políticas y procedimientos de seguridad cibernética de la empresa. Esto debe incluir la necesidad de que los empleados protejan las contraseñas o frases de acceso y el acceso a la computadora.	Una formación de calidad es importante para disminuir la vulnerabilidad a los ataques cibernéticos. Un programa de formación robusto en seguridad cibernética es por lo general aquel que se brinda al personal correspondiente en un entorno formal y no simplemente a través de correos electrónicos o memorandos.	Debe

ID	Criterios	Guía de la implementación	Debe / Debería
12.9	El personal que opera y administra los sistemas de tecnología de seguridad debe recibir capacitación sobre las operaciones y el mantenimiento en sus ámbitos específicos. Se acepta experiencia previa con sistemas similares. La autocapacitación a través de manuales operativos y otros métodos también se acepta.		Debe
12.10	El personal debe estar capacitado sobre cómo informar incidentes de seguridad y actividades sospechosas.	Los procedimientos para denunciar los incidentes de seguridad o actividades sospechosas son aspectos extremadamente importantes de un programa de seguridad, y la formación sobre cómo denunciar un incidente se puede incluir en la formación general de seguridad. Los módulos de formación especializados (que se basan en funciones laborales) pueden tener una formación más detallada sobre los procedimientos para hacer denuncias con el fin de que se incluyan detalles sobre el proceso: qué denunciar, a quién, cómo denunciarlo y qué hacer a continuación, después del informe.	Debe

Número de publicación: 1075-0420